

IN THE CLAIMS:

Set forth below in ascending order, with status identifiers, is a complete listing of all claims currently under examination. Changes to any amended claims are indicated by strikethrough and underlining. This listing also reflects any cancellation and/or addition of claims.

What is claimed is:

1. (currently amended) A method of using a firewall resident on a host computer to prevent spoofing of an address resolution cache of the host computer, the method comprising:

said firewall resident on the host computer receiving ~~an~~ a first unsolicited message from a ~~network~~ target computer station that submits a genuine new address resolution for a network protocol address;

said firewall checking independently cached address resolution information associated with the host computer;

in response to determining that cached address resolution information for said network protocol address of said target computer station has ~~an old~~ a previously cached address resolution which differs from said genuine new address resolution submitted by said first unsolicited message, said firewall issuing a first broadcast request for network elements having said network protocol address to reply with address resolution information in order to check the authenticity of the first unsolicited message submitting the genuine new address resolution for the network protocol address;

in response to determining that no reply messages match the previously cached ~~confirm~~ that a network element has said old address resolution that would contradict the genuine address resolution in the first unsolicited message, said firewall determining that said first unsolicited message is not spoofed and permitting at least one message to pass onto said host computer which includes said genuine new address resolution for said target computer station; ~~and~~

said firewall resident on the host computer receiving a second unsolicited message from a spoofer that submits a spoofed address resolution for the network protocol address of the target host computer;

said firewall checking the independently cached address resolution information associated with the host computer;

in response to determining that the previously cached address resolution information for said network protocol address differs from said spoofed address resolution submitted by said second unsolicited message, said firewall issuing a second broadcast request for network elements having said network protocol address to reply with address resolution information in order to check the authenticity of the second unsolicited message submitting the spoofed address resolution for the network protocol address of the target computer station;

in response to receiving a reply message from the target computer station that matches the previously cached ~~confirms a network element has said old~~ address resolution, said firewall determining that said second unsolicited message is a spoofed message and blocking at least one message which includes ~~include~~ said ~~new~~ spoofed address resolution from passing onto said host computer;

wherein said firewall resident in said host computer is operable to protect ~~protects~~ said host computer from spoofed address resolution messages while permitting genuine address resolutions.

2. (original) The method of claim 1, wherein said network implements a LAN network running Internet Protocol Version 4 using the Address Resolution Protocol (ARP) for resolving medium access control (MAC) addresses, and said address resolution cache is an ARP cache mapping IPv4 addresses to MAC addresses.

3. (original) The method of claim 1, wherein said network implements Internet Protocol Version 6 (IPv6) with Neighbor Discovery for resolving MAC addresses, and said address resolution cache is a Neighbor Discovery cache for mapping IPv6 addresses to MAC addresses.

4. (currently amended) A method of using a firewall resident on a host computer to prevent spoofing of an address resolution cache of the host computer, the method comprising:

said firewall resident on the host computer maintaining a shadow copy of said address resolution cache;

said firewall resident on the host computer receiving an unsolicited message from a network that submits a new address resolution for a network protocol address;

said firewall checking said shadow copy of said address resolution cache;

in response to determining that cached address resolution information for said network protocol address has an old address resolution which differs from said new address resolution submitted by said unsolicited message, said firewall issuing a request for network elements having said network protocol address to reply with address resolution information in order to check the authenticity of the unsolicited message submitting the new address resolution for the network protocol address;

in response to determining that no reply messages confirm that a network element has said old address resolution that would contradict the new address resolution of said unsolicited message, said firewall determining that said unsolicited message is not spoofed and permitting an update of said address resolution cache to have said new address resolution; and

in response to receiving a reply message that confirms a network element has said old address resolution in contradiction to said new address resolution of said unsolicited message, said firewall determining that said unsolicited message is spoofed and blocking an update of said address resolution cache to have said new address resolution;

wherein the validity of an unsolicited address resolution is checked by said firewall before permitting an update of said address resolution cache of said host computer.

5. (original) The method of claim 4, wherein said network implements a LAN network running Internet Protocol Version 4 using the Address Resolution Protocol (ARP) for resolving medium access control (MAC) addresses, and said address resolution cache is an ARP cache mapping IPv4 addresses to MAC addresses.

6. (original) The method of claim 4, wherein said network implements Internet Protocol Version 6 (IPv6) with Neighbor Discovery for resolving MAC addresses, and said address resolution cache is a Neighbor Discovery cache for mapping IPv6 addresses to MAC addresses.

7. (original) The method of claim 4, wherein said permitting said update of said address resolution cache comprises:

permitting a message having said new address resolution to pass onto a host computer.

8. (previously presented) The method of claim 4, wherein said blocking said update of said old address resolution comprises:

blocking at least one message having said new address resolution from passing onto a host computer.

9. (previously presented) The method of claim 4, wherein said maintaining said shadow copy comprises: storing cache entries with a residency lifetime greater than in said address resolution cache of said host computer.

10. (currently amended) A firewall resident on a host computer for preventing spoofing of an address resolution cache of the host computer, the firewall comprising:

a state machine in the firewall configured to check independently cached address resolution information in response to receiving an unsolicited address resolution response message directed to said host computer including a submitted new address resolution for a network protocol address;

said state machine generating a request for network elements to report an address resolution for said network protocol address in response to determining that said new address resolution of said unsolicited message differs from a previously cached address resolution for said network protocol address in order to check the authenticity of the unsolicited address resolution message submitting the new address resolution for the network protocol address;

said state machine permitting an update of cached address resolution information to include said submitted address resolution in response to determining that no address resolution reply messages have said previously cached address resolution for said network protocol address that would contradict the new address resolution of said unsolicited message; and

said state machine blocking an update of cached address resolution information of said address resolution cache of said host computer to include said submitted address resolution for said network protocol address in response to determining a reply message has said previously cached address resolution in contradiction to the new address resolution of said unsolicited message.

11. (previously presented) The firewall of claim 10, further comprising: a shadow copy of said address resolution cache, wherein said state machine is configured to check said shadow copy for cached address resolution information.
12. (original) The firewall of claim 11, wherein cache entries in said shadow copy have a residency lifetime greater than corresponding entries of said address resolution cache.
13. (original) The firewall of claim 10, wherein said address resolution cache is an ARP cache.
14. (original) The firewall of claim 10, wherein said address resolution cache is a Neighbor Discovery cache.
15. (cancelled)
16. (previously presented) The firewall of claim 10, wherein the firewall is resident on a chipset associated with a host computer.
17. (cancelled)
18. (previously presented) The method of claim 1, wherein the firewall is resident on a chipset associated with the host computer.
19. (cancelled)
20. (previously presented) The method of claim 4, wherein the firewall is resident on a chipset associated with the host computer.
21. (previously presented) The method of claim 1, wherein said cached address resolution information has an extended cache residency lifetime selected to support detection of spoofing attacks.

22. (previously presented) The method of claim 4, wherein said cached address resolution information is stored in a cache having an extended cache residency lifetime selected to support detection of spoofing attacks.

23. (previously presented) The firewall of claim 10, wherein said cached address resolution information is stored in a cache having an extended cache residency lifetime selected to support detection of spoofing attacks.